Matt Stark – Individual Contributions

For my individual contribution, I developed a security system and login/register system designed around user privacy concerns and security.

When a user registers, they are given a unique user code but this code is not stored on the server. The user code is added with the user’s postcode and encrypted and salted. This ensures that no amount of hacking of the database can retrieve a user’s unique code. This means that users worried about security can be at rest.

Other security features implemented include:

* All endpoints are secured behind JWT tokens that MUST be generated on the server to be accepted before an endpoint can be accessed.
* Tokens have expiry dates that after they expire can no longer be used
* There is a 2-tier login system to ensure that a user can only communicate with the constituency server they are based in as each server uses unique secret keys.
* DDOS protection is in place per constituency.
  + This means that each constituency has its own dedicated server, with its URL private and secure behind encrypted JWT tokens. If a server is taken down, it only takes down a single constituency and it can be restarted really easily.
* Replicating server hosting with multiple ‘pods’ when required to horizontally scale for demand
* Rejected web requests from any JWT token not created on the server

The separation of everything into APIs was also my own individual contribution and its abstracted calls to the database away from the Frontend.

The addition of Mongoose to talk to our mongo database, enforcing schema and subdocuments on our data to ensure consistency, was also an individual contribution.